UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/971,717	10/04/2001	David Ian Houlding	92717-319	3038

7590 02/08/2007

Gary B. Solomon
Jenkens & Gilchrist, P.C.
3200 Fountain Place
1445 Ross Avenue
Dallas, TX 75202-2799

EXAMINER	
SHIFERAW, ELENI A	
ART UNIT	**PAPER NUMBER**
2136	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	02/08/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	09/971,717	HOULDING, DAVID IAN	
	Examiner	Art Unit	
	Eleni A. Shiferaw	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 November 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-13,15-22 and 24-30* is/are pending in the application.

4a) Of the above claim(s) *14 and 23* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-13,15-22 and 24-30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 11/17/2006 has been entered.

Response to Amendment

2. Applicant amendments and arguments are moot in view of new grounds of rejection.

3. Claims 1-13, 15-22, and 23-30 are currently pending.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-13, 15-22, and 24-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cunningham et al. Pub. No.: US 2005/0086295 A1 in view of Wesinger, Jr. et al.

Regarding claims 1 and 26, Cunningham et al. teaches a method/system for providing security (fig. 2 element 21) to a client computing system (fig. 2 element 11) in communication with a host communication system across a network (fig. 2 element 31), said method comprising:

executing a browser on the client computing system (0022; *client web browser is executed*);

communicating, from the client to the host computing system, a request to download data to be displayed in the browser (0027-0028, 0035 and 0031);

downloading the data from the host computing system to the client computing system via a client side firewall in response to the download request (fig. 4; *downloading real-time data to client computing system via client firewall as shown on fig. 2 element 21, from the server based on client request*);

loading an interactive software application in the browser, the interactive software application utilizing the data downloaded from the host computing system (claim 1, 0029, and 0032; *asynchronous hypertext messages encoded in said HTML document*);

executing the interactive software application in the browser on the client computing system, the interactive software application being in communication with at least one element that is **outside the browser** (0051-0052; ***the browser communicating with user device system that is outside the browser***) and on the client side behind the client side firewall (0051-0052; *the hypertext message in HTML document sent from server to client is executed/displayed on the client computing system in communication with the client system in communication with the client side firewall*); and

wherein the communication between the interactive software application and the at least one element occurs after the loading of the interactive software application (0010-0013; *the application received and displayed is in communication with the client underlying architecture system*).

Cunningham et al. fails to explicitly disclose wherein the communication between the interactive software application and the at least one element occurs exclusively on the client side of the client side firewall. However Wesinger, Jr. et al. discloses a client side firewall (fig. 3 element 305) authenticating and/verifying verifying exclusively on the client side firewall, with stored rules (fig. 3 element 316 and 321) stored in the firewall, for a user (fig. 3 elements 305A, 305B) connection request received from a user browser (col. 9 lines 48-67).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the teachings of Wesinger, Jr. et al. within the system of Cunningham et al. because they are analogous in firewall authentication. One would have been motivated to modify the teachings of Wesinger, Jr. et al. within the system because it would save processing time by verifying some data inside the client side firewall instead of web server authenticating each users especially when lots of user requests are received at the same time.

Regarding claim 12, Cunningham et al. discloses a system for providing security to a client computing system operating a browser in communication with an interactive software application maintained by a host computing system (figs. 2-5), said system comprising:

at least one processor in the client computing system operable to generate and communicate a request to download the interactive software application from the host computing system to the client computing system (0027-0028, and 0031);

a memory operating in the client computing system to store the interactive software application downloaded in response to the download request, said at least one processor executing the stored interactive software application inside the browser on the client computing system, the executed interactive software application and the browser being in communication with at least one element (fig. 4; *downloading real-time data to client computing system memory storage via client firewall as shown on fig. 2 element 21, from the server based on client request*) that is **outside the browser and on the client side of the client side firewall** (0051-0052; ***the browser communicating with user device system that is outside the browser***);

wherein the communication between the interactive software application and the at least one element occurs after the loading of the interactive software application (0010-0013; *the application received and displayed is in communication with the client underlying architecture system*).

Cunningham et al. fails to explicitly disclose wherein the communication between the interactive software application and the at least one element occurs exclusively on the client side of the client side firewall. However Wesinger, Jr. et al. discloses a client side firewall (fig. 3 element 305) authenticating and/verifying verifying exclusively on the client side firewall, with stored rules (fig. 3 element 316 and 321) stored in the firewall, for a user (fig. 3 elements 305A, 305B) connection request received from a user browser (col. 9 lines 48-67).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the teachings of Wesinger, Jr. et al. within the system of Cunningham et al. because they are analogous in firewall authentication. One would have been motivated to modify the teachings of Wesinger, Jr. et al. within the system because it would save processing time by verifying some data inside the client side firewall instead of web server authenticating each users especially when lots of user requests are received at the same time.

Regarding claim 19, Cunningham et al. discloses a method for providing security to a client computing system operating an interactive software application (figs. 2-5), said method comprising:

loading the interactive software application on the client computing system (fig. 4; *downloading real-time data to client computing system via client firewall as shown on fig. 2 element 21, from the server based on client request*);

executing the interactive software application on the client computing system (0051-0052; *the hypertext message in HTML document sent from server to client is executed/displayed on the client computing system in communication with the client system*);

communicating a digital signature to the browser (0034, 0038, 0058 TABLE 1, and 0065; *signature/certificate authentication*);

verifying digital signature (0034, 0038, 0058 TABLE 1, and 0065; *signature/certificate authentication and verification*);

upon confirmation of the digital signature, opening a port of the browser for receiving data from at least one element (fig. 4 element S8-S9 and 0034-0052; *authenticating based on*

signature and opening port to provide data) that is **outside the browser and on the client side of the client side firewall** (0051-0052; ***the browser communicating with user device system that is outside the browser***); and

communicating data between the at least one element and the browser on the client computing system (0051-0052; *the hypertext message in HTML document sent from server to client is executed/displayed on the client computing system in communication with the client system*).

Cunningham et al. fails to explicitly disclose wherein the communication between the interactive software application and the at least one element occurs exclusively on the client side of the client side firewall. However Wesinger, Jr. et al. discloses a client side firewall (fig. 3 element 305) authenticating and/verifying verifying exclusively on the client side firewall, with stored rules (fig. 3 element 316 and 321) stored in the firewall, for a user (fig. 3 elements 305A, 305B) connection request received from a user browser (col. 9 lines 48-67).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the teachings of Wesinger, Jr. et al. within the system of Cunningham et al. because they are analogous in firewall authentication. One would have been motivated to modify the teachings of Wesinger, Jr. et al. within the system because it would save processing time by verifying some data inside the client side firewall instead of web server authenticating each users especially when lots of user requests are received at the same time.

Regarding claims 2 and 13, Cunningham et al. discloses the method/system wherein the communication includes issuing and receiving events (claim 1).

Regarding claims 3 and 14, Cunningham et al. discloses the method/system wherein the at least one element includes at least one of a browser and an element of an underlying architecture (0035-0052).

Regarding claims 4 and 15, Cunningham et al. discloses the method/system wherein the interactive software application is an applet (claim 5 and 0064);

Regarding claim 5 Cunningham et al. discloses the method/system wherein the applet is Java applet (claim 5 and 0064);

Regarding claims 6, 16 and 22, Cunningham et al. discloses the method/system wherein the communication commences after verification of a digital signature (0034, 0038, 0058 TABLE 1, and 0065);

Regarding claim 7, Cunningham et al. discloses the method/system further comprising:

reading a digital signature (0034, 0038, 0058 TABLE 1, and 0065; *reading it to authenticate*);

verifying the digital signature (0034, 0038, 0058 TABLE 1, and 0065; *certificate/signature authentication*); and

opening a port of the browser to receive events from the at least one element (fig. 4 element S8-S9 and 0034-0052; *authenticating based on signature and opening port to provide data*).

Regarding claims 8 and 17, Cunningham et al. discloses the method/system wherein the data includes a model representative of an underlying architecture of a software system (0030, and 0028).

Regarding claim 10, Cunningham et al. discloses the method/system wherein the data includes content and format information (0035-0052).

Regarding claims 11, 18 and 25, Cunningham et al. discloses the method/system wherein the browser is a web browser (claim 22 and fig. 2 element 51).

Regarding claim 20, Cunningham et al. discloses the method/system wherein the data includes at least one of events and requests (0058 TABLE 1).

Regarding claim 21, Cunningham et al. discloses the method/system wherein the events and requests utilize the HTTP protocol (claim 31).

Regarding claim 24, Cunningham et al. discloses the method/system wherein the at least one element operates on the client side of the client firewall (0024).

Regarding claims 27-30, Cunningham et al. discloses the method/system wherein the at atleast one element is operating on the client computing system includes a component of an underlying architecture of the client computing system (0010-0013; *the application received and displayed is in communication with the client underlying architecture system*).

Conclusion

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Eleni A. Shiferaw whose telephone number is 571-272-3867. The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser R. Moazzami can be reached on (571) 272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

February 2, 2007

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

2/3/07